REMOTE ACCESS POLICY

INTRODUCTION

The purpose of this policy is to define standards for connecting to Alabama Department of Postsecondary Education's (DPE) network from any host. These standards are designed to minimize the potential exposure to DPE from damages which may result from unauthorized use of DPE resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical DPE internal systems, etc.

1.0 POLICY

1.1 Only selected staff members of the Division of Information Services and authorized third parties (consultants, vendors, etc...) may, under some circumstances, utilize remote access to access DPE computing resources for which they have been granted access.

1.1.1 Contractors, vendors, or agents with remote access privileges must have prior approval of the Director of Information Systems before logging into DPE systems for any reason.

1.1.2 Contractors, vendors, and agents shall not make any unauthorized changes to programs, applications, data, system configurations, or any other resource.

1.2 Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

1.3 It is the responsibility of DPE employees, contractors, vendors and agents with remote access privileges to DPE network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

1.3.1 At no time should any staff member provide their login or email password to anyone, not even family members.

1.3.2 Employees and contractors with remote access privileges must ensure that their DPE owned or personal computer or workstation, which is remotely connected to the network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

1.3.3 All hosts that are connected to internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

1.4 All hosts connecting to internal system not generally available to all internet users will connect through a VPN session through the firewall managed by Alabama Supercomputer Authority.

1.5 Only supported remote control software will be allowed to communicate from the VPN server to internal hosts unless specifically requested and approved. Currently Microsoft Remote Desktop is supported.

1.6 A log of all remote access sessions shall be kept and reviewed and on a weekly basis by the Network Administrator.